Securing Your Data with the PCI Data Security Standard

The largest credit card heist in history

In January 2009, Heartland Payment Systems disclosed a security breach that may have exposed as many as 100 million credit card numbers. Heartland is the largest credit card processing house in the world, and this loss took place even though the company had been audited and certified compliant with the Payment Card Industry (PCI) Data Security Standard (DSS) only the previous April.

What does this have to do with me?

If you process credit card transactions, take online credit card payments, or store or handle credit card information on paper, online, or over the phone, your merchant agreement requires you to be in compliance, and you've agreed to be fined $25 per cardholder disclosed if you have a security breach.

Even if you don't handle credit cards, but you do store confidential business materials, keep information on your customers, or maintain personnel and payroll records, the PCI DSS provides valuable guidance and lessons that can help your organization. The PCI DSS reflects a worldwide industry consensus regarding how to protect sensitive data.

A comprehensive data security standard

The PCI DSS is a set of requirements designed by the PCI Security Standards Council to protect cardholder information. The Council includes representatives from every credit card company you've ever heard of, worldwide. It's somewhat unique in that it's an information security regulation that's not mandated by a government entity. The standard is designed to protect customer information, and it includes requirements for security management, policies, procedures, network architecture, software design, and more.

Business organizations tend to worry about return on investment. Reflecting that concern, the PCI DSS includes a set of priorities that help you to address the low-hanging fruit first, helping you get the most out of your security investment.

Data security requirements

The PCI DSS standard dictates straightforward, bread-and-butter steps to protect data — steps that we can all agree with, including:

- *Build and maintain a secure network.* Use a firewall, and don't use default passwords on network devices or systems.
- *Protect cardholder data.* Protect it when stored, and protect it when in motion through the use of encryption as well as logical and physical access controls.
- *Manage vulnerabilities.* Maintain secure systems and applications. Use and also update antivirus software.
- *Implement strong access-control measures.* Restrict physical and online access on a need-to-know basis. Don't allow sharing of user IDs; have one per person per login so that you have accurate audit trails.
- *Monitor and test.* Track and log all access to network resources and cardholder data. Test security systems and processes.
- *Maintain an information security policy.* Use this document to guide both your operations and your developers that create new applications and ways to handle cardholder data.

A prioritized list

Just as important as the complete list of requirements you'll find in the standard is the fact that the PCI DSS prioritizes compliance efforts by listing specific milestones to accomplish (see Table 1). Although the data security standards contain no surprises, the

Milestone	Goals
1	*Remove sensitive authentication data and limit data retention.* From experience, a big risk is storing data that doesn't need to be stored. The less sensitive information you store, the smaller the risk.
2	*Protect your perimeter, internal, and wireless networks.* Most successful security breaches have used one of these three vectors for the attack.
3	*Secure payment card applications.* Applications themselves are often vulnerable, and they should be designed, developed, and audited to protect against this mode of attack.
4	*Monitor and control access to your systems.* Your systems should allow you to detect who, what, when, and how someone accesses a network or system containing cardholder data.
5	*Protect stored cardholder data.* Restrict physical access and online access, and encrypt data at rest.
6	*Finalize compliance efforts and ensure that all controls are in place.* Make sure that all of the standard's remaining policies, procedures, and processes are implemented.

Table 1: PCI DSS prioritizes compliance efforts by listing specific milestones to accomplish.

READ ABOUT *the PCI Security Standards Council's prioritized approach at:*
https://www.pcisecuritystandards.org/education/prioritized.shtml

priority list is remarkable in how highly it ranks the importance of application security. Applications, whether used internally or externally, whether web-based or hard-coded, often provide the onramp for hackers to compromise your data. Buffer overflow, SQL injection, URL parameter manipulation, and cookie poisoning are just a few exploits to which applications can be vulnerable. The PCI DSS suggests that applications need to be developed with security in mind, but then audited and monitored.

The moral of the story

The Heartland story serves as a sobering reminder of how deeply you can get into trouble if you fail to actually implement a good data security standard. This story applies to you whether you handle credit card data or just need to keep your product plans and employee Social Security information and birthdates a secret.

What is worrisome about the Heartland story is that the company endured the largest loss of cardholder data in history despite the fact that it was certified compliant with the PCI DSS. According to Heartland, so far the breach has cost the company $12.6 million, including a $6 million fine by MasterCard.

We believe that the PCI DSS is an excellent standard, and that following its provisions can greatly improve the security of your environment. But beware that all certification reviews aren't created equally. All too often, security auditors work by completing a checklist. They may interview your staff about your security infrastructure, but then fail to audit whether you actually implemented what you said you did. Is data really encrypted in transit? Is that firewall configured correctly, and is it actually plugged into the right networks? A thorough security review requires this and more — it requires in-depth technical examination, and critical thinking about systems, processes, and dataflow within your environment.

Your data security is only as good as your actual *implementation*. Whether you are pursuing PCI DSS compliance, or protecting other sensitive data, you need to make sure that your environment's design and implementation is examined with a critical, technical eye. This means that you need assistance from experts that really understand both the technology and the intent of the standard, and don't solely work from a checklist. Applied Trust prides itself on performing in-depth, technical analysis of our clients' environments. ■

This article was reprinted from the Q4 2009 issue of The Barking Seal, a publication of Applied Trust. You can subscribe to The Barking Seal online at http://www.appliedtrust.com/barkingseal.